

# METHOD AND SYSTEM FOR INPUT/OUTPUT INFORMATION MANAGEMENT OF DIGITAL CONTENTS, AND RECORDING MEDIUM WITH PROGRAM RECORDED FOR INPUT/OUTPUT MANAGEMENT OF DIGITAL CONTENTS

Publication number: JP2002007263

Publication date: 2002-01-11

Inventor: MUROTA SHOJI; ASANO MAKI; ARAKI HIDENORI

Applicant: NTT COMM KK

Classification:

- international: G06K19/07; G06F12/14; G06F13/00; G06F15/00; G06F21/06; G06F21/20; G06F21/24; G06K17/00; G06Q10/00; G06Q50/00; G09C1/00; H04L9/10; H04L9/32; G06K19/07; G06F12/14; G06F13/00; G06F15/00; G06F21/00; G06F21/20; G06K17/00; G06Q10/00; G06Q50/00; G09C1/00; H04L9/10; H04L9/32; (IPC1-7): G06F13/00; G06F15/00; G06F17/60; G06K17/00; G06K19/07; G09C1/00; H04L9/10; H04L9/32

- European:

Application number: JP20000193360 20000627

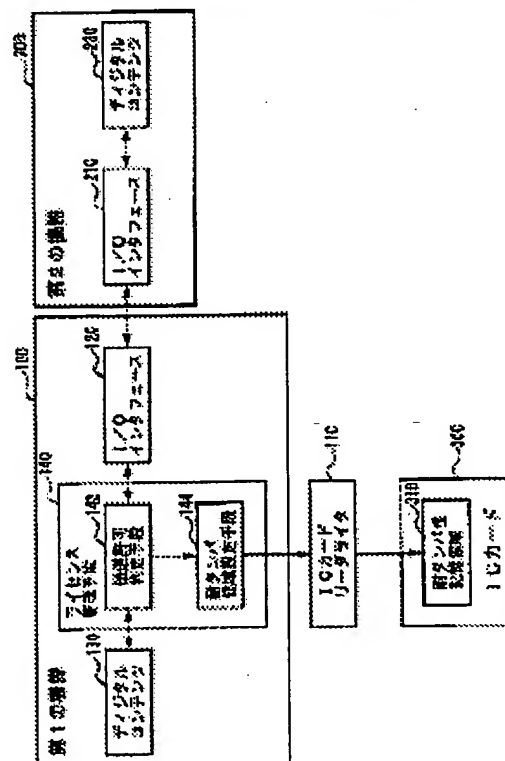
Priority number(s): JP20000193360 20000627

Report a data error here

## Abstract of JP2002007263

**PROBLEM TO BE SOLVED:** To provide a method and a system for digital contents management which reduces the risk of a tamper-resistant area being broken, uses a terminal other than a terminal used for downloading as a contents storage and management terminal, and changes the contents storage, and to provide management terminal for one contents. **SOLUTION:** Individual equipment, having a tamper-resistant storage area provided with an area where input/output information of digital contents transmitted between devices is stored, is connected to one of the devices transmitting the digital contents and input/output information of the digital contents to the device, where the equipment is connected is written to the tamper-resistant storage area of the equipment.

本発明によるデジタルコンテンツ  
入出力情報管理システムの構成図



Data supplied from the esp@cenet database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2002-7263  
(P2002-7263A)

(43) 公開日 平成14年1月11日 (2002.1.11)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テマコード (参考)
G 0 6 F 13/00	5 4 0	G 0 6 F 13/00	5 4 0 S 5 B 0 3 5
15/00	3 3 0	15/00	3 3 0 A 5 B 0 4 9
17/60	1 4 2	17/60	1 4 2 5 B 0 5 8
	5 1 0		5 1 0 5 B 0 8 5
	5 1 2		5 1 2 5 J 1 0 4

審査請求 未請求 請求項の数 8 O L (全 12 頁) 最終頁に続く

(21) 出願番号 特願2000-193360 (P2000-193360)

(22) 出願日 平成12年6月27日 (2000.6.27)

(71) 出願人 399035766

エヌ・ティ・ティ・コミュニケーションズ  
株式会社  
東京都千代田区内幸町一丁目1番6号

(72) 発明者 室田 将司

東京都千代田区内幸町一丁目1番6号 エ  
ヌ・ティ・ティ・コミュニケーションズ株  
式会社内

(74) 代理人 100070150

弁理士 伊東 忠彦

最終頁に続く

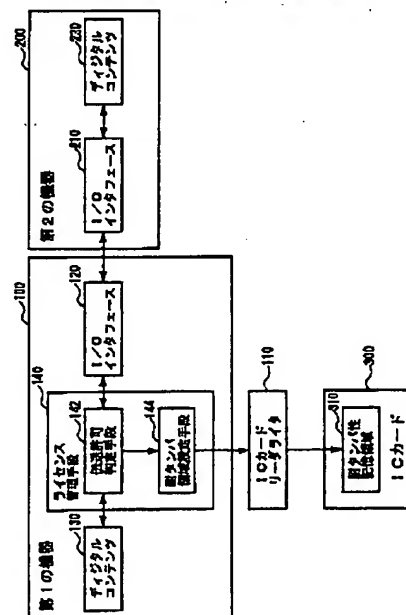
(54) 【発明の名称】 デジタルコンテンツの入出力情報管理方法及び管理システム、並びに、デジタルコンテンツの入出力情報管理用プログラムを記録した記録媒体

(57) 【要約】

【課題】 本発明は、耐タンパ領域が破られる危険性が減少され、ダウンロードに利用された端末以外の端末をコンテンツ蓄積・管理端末として利用できるようにされ、一つのコンテンツに対するコンテンツ蓄積・管理端末を変更できるようにされたデジタルコンテンツ管理方法及びシステムの提供を目的とする。

【解決手段】 本発明は、機器間で伝送されるデジタルコンテンツの入出力情報を格納する領域が設けられた耐タンパ性記憶領域を有する別個の装置を、デジタルコンテンツが伝送されるいずれか一方の機器に接続し、装置が接続された一方の機器に対するデジタルコンテンツの入出力情報を装置の耐タンパ性記憶領域に書き込むことを特徴とする。

本発明によるデジタルコンテンツ  
入出力情報管理システムの構成図



## 【特許請求の範囲】

【請求項 1】 機器間で伝送されるデジタルコンテンツの入出力情報を管理する方法であって、

上記デジタルコンテンツの上記入出力情報を格納する領域が設けられた耐タンパ性記憶領域を有する別個の装置を、上記デジタルコンテンツが伝送されるいずれか一方の機器に接続し、  
上記機器間での上記デジタルコンテンツの入出力情報を上記装置の上記耐タンパ性記憶領域に書き込むことを特徴とする方法。

【請求項 2】 第 1 の機器から第 2 の機器に伝送されるデジタルコンテンツの入出力情報を管理する方法であって、

上記デジタルコンテンツの上記入出力情報を格納する領域が設けられた耐タンパ性記憶領域を有する別個の装置を上記第 1 の機器と第 2 の機器の少なくともいずれか一方の機器に接続し、

上記第 1 の機器から上記第 2 の機器への上記デジタルコンテンツの伝送が許可されているかどうかを判定し、  
上記デジタルコンテンツの伝送が許可されている場合に、上記デジタルコンテンツを上記第 1 の機器から上記第 2 の機器に伝送し、上記デジタルコンテンツが上記機器間で伝送されたことを示す上記入出力情報を上記別個の装置の上記耐タンパ性記憶領域に書き込むことを特徴とする方法。

【請求項 3】 上記装置として IC カードが利用され、  
上記 IC カードは IC カードリーダーを介して上記一方の機器に接続されることを特徴とする請求項 1 又は 2 記載の方法。

【請求項 4】 上記一方の機器はデジタルコンテンツ提供端末であることを特徴とする請求項 1 乃至 3 のうちいずれか一項記載の方法。

【請求項 5】 上記一方の機器は携帯型情報端末であることを特徴とする請求項 1 乃至 3 のうちいずれか一項記載の方法。

【請求項 6】 上記一方の機器は上記デジタルコンテンツを蓄積するユーザ端末であることを特徴とする請求項 1 乃至 3 のうちいずれか一項記載の方法。

【請求項 7】 第 1 の機器と第 2 の機器の間で伝送されるデジタルコンテンツの入出力情報を管理するシステムであって、

上記第 1 の機器に接続された IC カードリーダーと、

上記 IC カードリーダーに挿入され、上記デジタルコンテンツの上記入出力情報を格納する領域が設けられた耐タンパ性記憶領域を有する IC カードとを更に有し、

上記 IC カードリーダーが接続された上記第 1 の機器は、上記デジタルコンテンツの不正使用を防止するライセンス管理手段を有し、

上記ライセンス管理手段は、上記第 1 の機器と上記第 2 の機器の間の上記デジタルコンテンツの伝送が許可されているかどうかを判定する手段と、

許可されていると判定された場合に、上記デジタルコンテンツの伝送を始動させ、上記デジタルコンテンツの伝送に応じた入出力情報を上記 IC カードリーダーを介して上記 IC カードの耐タンパ性領域に設定する手段とを有することを特徴とするシステム。

【請求項 8】 デジタルコンテンツを保持する第 1 の機器と、上記第 1 の機器から上記デジタルコンテンツを受ける第 2 の機器と、上記第 1 の機器と上記第 2 の機器の少なくとも一方の機器に接続された IC カードリーダーと、上記 IC カードリーダーに挿入され、上記デジタルコンテンツの上記入出力情報を格納する領域が設けられた耐タンパ性記憶領域を有する IC カードとを有するシステムにおいて、上記一方の機器で実行されるデジタルコンテンツの入出力情報管理プログラムを記録した記録媒体であって、  
上記第 1 の機器から上記第 2 の機器への上記デジタルコンテンツの伝送が不正使用であるかどうかを判定させるコードと、

不正使用ではないと判定された場合に、上記デジタルコンテンツの伝送を始動させ、上記デジタルコンテンツの伝送に応じた入出力情報を上記 IC カードリーダーを介して上記 IC カードの耐タンパ性領域に設定させるコードとを有し、上記デジタルコンテンツの不正使用を防止することを特徴とするプログラムを記録した記録媒体。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、デジタルコンテンツ提供情報端末、携帯型端末、デジタルコンテンツ蓄積・利用装置、デジタルコンテンツ利用装置などの機器間で流通されるデジタルコンテンツを管理する方法及びシステム、並びに、管理用プログラムを記録した記録媒体に関する。

## 【0002】

【従来の技術】従来より、著作権保護の必要があるデジタルコンテンツ、たとえば、音楽コンテンツ、映画コンテンツ、ソフトウェアコンテンツなどでは、デジタルコンテンツの著作権を守るために様々な業界団体がコンテンツの扱いに規定を設けることによって著作権保護の指針を示す役割を担っている。

【0003】たとえば、音楽コンテンツの場合、SDMI (Secure Digital Music Initiative) という団体が LCM (Licensed Compliant Modules) をゲートウェイにして、コンテンツのチェックアウト/チェックイン (すなわち、コンテンツ利用機器やコンテンツ蓄積機器へのコンテンツの出し入れ) を、耐タンパ性 (すなわち、物理的攻撃、改竄などに対する抵抗性) をもつ領域 (たとえ

ば、記憶領域)で管理するという方針を打ち出している。

【0004】正当な手続・手段で取得されたオリジナルの音楽コンテンツは、コンテンツが取得された機器内にある耐タンパ領域で安全、機密的に管理されることが要請される。

【0005】LCMは、具体的には、デジタルコンテンツのコピー、あるいは、デジタルコンテンツの移動(蓄積場所の変更)に関してメディアに応じて制限を加え、その制限の範囲内でデジタルコンテンツを正当に利用できるようにする。

【0006】図1乃至4を参照して、このLCMの規定に準拠した従来の音楽コンテンツ取得システムの例を説明する。図1は、CDに記録された音楽コンテンツをCDから取り出し、形式変換して利用・蓄積するCDリッピングの例の説明図である。

【0007】パーソナルコンピュータ10は、CD-Romドライブ11に搭載されたCD-Romから音楽コンテンツを読み出し、形式変換部12によってコンピュータが利用できる圧縮形式に音楽コンテンツを形式変換(CDリッピング)する。形式変換された音楽コンテンツは、LCMの規定に従って、蓄積装置16に蓄積され、あるいは、I/Oインタフェース17を介して外部の利用機器30に移される。LCMの規定に従った音楽コンテンツの取り扱いを行なうため、パーソナルコンピュータ10内のハードディスク上若しくはICチップ上に耐タンパ領域15を設け、コンテンツ管理用アプリケーションモジュール14と、ライセンス・コンプライアント・モジュール(LCM)とを利用して、音楽コンテンツのチェックイン/チェックアウトを管理する。このように、CDリッピングを行なうパーソナルコンピュータ10は、音楽コンテンツの蓄積用端末、並びに、管理用端末として働く。音楽コンテンツは、パーソナルコンピュータ10の蓄積装置16だけではなく、たとえば、メモリメディアのような記録媒体にも蓄積することが可能であり、そのため、パーソナルコンピュータ10は、このようなメモリメディアのためのメディアドライブ18を具備する。

【0008】利用機器30は、たとえば、プレーヤーのような機器であり、I/Oインタフェース31を介してパーソナルコンピュータ10から送られる音楽コンテンツを受信し、記録媒体32に一時的に記憶すると共に、その音楽コンテンツを再生する。また、一般的に、パーソナルコンピュータ10から利用機器30への音楽コンテンツの配信のような機器間におけるデジタルコンテンツの伝送の際に、デジタルコンテンツは、不正利用を防止するため、公知の暗号化方式を利用して伝送される。

【0009】図2は、ネットワーク経由でコンテンツをダウンロードするシステムの構成図である。この例で

は、パーソナルコンピュータ10は、コンピュータネットワーク50などのネットワーク及びネットワークインタフェース19を介してコンテンツサーバー40からコンテンツをダウンロードし、蓄積装置16に蓄積する。たとえば、パーソナルコンピュータ10が、図1の例と同様に音楽コンテンツをネットワーク50経由で取得した場合、パーソナルコンピュータ10は、ハードディスク上若しくはICチップ上に耐タンパ領域15を設け、コンテンツ管理用アプリケーションモジュール14とLCM13とを利用することによって、個人所有のコンテンツ蓄積・管理用端末として働き、コンテンツのチェックイン/チェックアウト管理を行なうことができる。

【0010】図3は、コンテンツ提供情報端末を利用してコンテンツを取得するシステムの構成図である。コンテンツ提供情報端末60、たとえば、KIOSK端末(公共的なスペースに設置され、利用者が自分で操作してコンテンツ取得、情報検索などを行なうことができる端末)は、蓄積装置61に蓄積された音楽コンテンツ、若しくは、メディアドライブ66を介してメディアから取り込んだ音楽コンテンツを、I/Oインタフェース65を介して接続された利用機器30にダウンロードする。コンテンツ提供情報端末60は、ハードディスク上若しくはICチップ上に耐タンパ領域62を設け、コンテンツアプリケーションモジュール63及びLCM64を利用することによって、コンテンツのチェックイン/チェックアウト管理を行なうことができる。

【0011】コンテンツ提供情報端末60に接続され、コンテンツ提供情報端末60からコンテンツを取得する携帯型の利用機器30は、取得したコンテンツを記録媒体32に記録し、あるいは、コンテンツを再生する機器である。しかし、利用機器30自体は、コンテンツを蓄積、管理する能力を具備しない。そこで、利用機器30の記録媒体32に記録されたコンテンツは、I/Oインタフェース31を介してパーソナルコンピュータ10のようなコンテンツ蓄積・管理用端末に転送され、待避される。そのため、コンテンツ提供情報端末60上のLCM64及びパーソナルコンピュータ10上のLCM13は、コンテンツ提供情報端末60から取得されたコンテンツが、携帯型利用機器30などの記録媒体32からパーソナルコンピュータ10などのコンテンツ蓄積・管理用端末に1回に限り待避できるように変更される。これにより、ユーザが所望のコンテンツ蓄積・管理用端末10でチェックイン/チェックアウト管理を行なえるようにする方法も提案されている。

【0012】図4は、携帯端末を利用してコンテンツサーバーからコンピュータネットワークのようなネットワークを介してコンテンツをダウンロードするシステムの構成図である。コンテンツは、コンテンツサーバー40からコンピュータネットワーク50のようなネットワークを介して携帯端末70にダウンロードされる。携帯端

末 70 は、ネットワークインタフェース 71 によって受信されたコンテンツを記録媒体 73 に記録することができる。携帯端末 70 として、たとえば、携帯電話機や PDA が使用される。本例の場合に、音楽コンテンツがダウンロードされる携帯端末 70 は、コンテンツの蓄積・管理用端末ではないため、図 3 の例と同様に、音楽コンテンツは、情報端末 70 から I/O インタフェース 72 を介してパーソナルコンピュータ 10 に送信される。パーソナルコンピュータ 10 は、ハードディスク上若しくは IC チップ上に耐タンパ領域 15 を設け、コンテンツ管理用アプリケーションモジュール 14 と LCM 13 とを利用することによって、個人所有のコンテンツ蓄積・管理用端末として働き、コンテンツのチェックイン/チェックアウト管理を行なうことができる。

【0013】以上のように、従来技術の場合、コンテンツのチェックイン/チェックアウトはコンテンツ蓄積・管理用端末で行なわれる。

【0014】

【発明が解決しようとする課題】図 1 並びに図 2 に示された従来のシステムの場合、コンテンツは、パーソナルコンピュータ 10 のようなコンテンツのダウンロード兼蓄積用端末に取り込まれるので、このコンテンツのチェックイン/チェックアウト管理は、コンテンツがダウンロードされる端末で行なわれ、耐タンパ領域はダウンロード兼蓄積・管理用端末に設けられている。しかしながら、ダウンロード兼蓄積・管理用端末には寿命があり、かつ、従来技術では、耐タンパ領域からの管理データの移動は許されていない。そのため、ダウンロード兼蓄積・管理用端末の寿命が来ると、本来寿命は無い筈のコンテンツも寿命になり、端末が使えなくなるとコンテンツも使えなくなるといった問題点がある。さらに、ダウンロード兼蓄積・管理用端末の耐タンパ領域は、メモリ上にソフトウェア的手法で設けられるので、不正な手段で破られる可能性が高いという問題点がある。

【0015】また、図 3 並びに図 4 に示された従来技術の場合、コンテンツを取得する機器、すなわち、利用機器 30 又は携帯端末 70 と、コンテンツを蓄積・管理する機器、すなわち、パーソナルコンピュータ 10 とが異なる装置であり、コンテンツを取得した機器内の耐タンパ領域でコンテンツのチェックイン/チェックアウト管理を行なうという原則を保持することが難しい。

【0016】さらに、図 1 乃至 4 に示された従来技術の例の場合に共通して、コンテンツの蓄積管理用機器内でチェックイン/チェックアウトの管理がなされるので、コンテンツの出し入れ等の著作権に係る編集操作は、蓄積管理用機器以外では行なえなくなり、ユーザにとって極めて不便である。

【0017】上記の従来技術の問題点に鑑みて、本発明は、耐タンパ領域が破られる危険性が減少され、ダウンロードに利用された端末以外の端末をコンテンツ蓄積・

管理端末として利用できるようにされ、かつ、一つのコンテンツに対するコンテンツ蓄積・管理端末を変更できるようにされたデジタルコンテンツを管理する方法及びシステム、並びに、管理用プログラムを記録した記録媒体の提供を目的とする。

【0018】

【課題を解決するための手段】上記本発明の目的を達成するため、請求項 1 に係る発明は、機器間で伝送されるデジタルコンテンツの入出力情報を管理する方法であって、上記デジタルコンテンツの上記入出力情報を格納する領域が設けられた耐タンパ性記憶領域を有する別個の装置を、上記デジタルコンテンツが伝送されるいずれか一方の機器に接続し、上記機器間での上記デジタルコンテンツの入出力情報を上記装置の上記耐タンパ性記憶領域に書き込むことを特徴とする。

【0019】請求項 2 に係る発明は、第 1 の機器から第 2 の機器に伝送されるデジタルコンテンツの入出力情報を管理する方法であって、上記デジタルコンテンツの上記入出力情報を格納する領域が設けられた耐タンパ性記憶領域を有する別個の装置を上記第 1 の機器と第 2 の機器の少なくともいずれか一方の機器に接続し、上記第 1 の機器から上記第 2 の機器への上記デジタルコンテンツの伝送が許可されているかどうかを判定し、上記デジタルコンテンツの伝送が許可されている場合に、上記デジタルコンテンツを上記第 1 の機器から上記第 2 の機器に伝送し、上記デジタルコンテンツが上記機器間で伝送されたことを示す上記入出力情報を上記別個の装置の上記耐タンパ性記憶領域に書き込むことを特徴とする。

【0020】請求項 1 並びに請求項 2 に係る発明によれば、実際にデジタルコンテンツがダウンロードされ、あるいは、蓄積される機器とは別個の装置にデジタルコンテンツの入出力情報を格納する領域が設けられるので、格納領域が不正にアクセスされる危険性が低減する。また、機器間でデジタルコンテンツの伝送を行なう際に、この別個の装置が接続されているいずれか一方の機器からデジタルコンテンツの入出力情報を書き込むことができるので、ダウンロードされ、蓄積される側ではない方の機器を一方の機器として選択することによって、ダウンロードに利用された端末以外の端末をコンテンツ蓄積・管理端末として利用できるようになる。また、デジタルコンテンツを伝送する際に、そのデジタルコンテンツについての入出力情報を別個の装置に書き込むために直前に使用された機器とは異なる機器にその別個の装置を接続し、今回の伝送に関する入出力情報をその別個の装置に書き込むことによって、一つのコンテンツに対するコンテンツ蓄積・管理端末を変更することが可能である。

【0021】また、請求項 3 に係る発明によれば、上記装置として IC カードが利用され、上記 IC カードは I

Cカードリーダーライタを介して上記一方の機器に接続される。したがって、ICカードに本質的に備わっている安全性を有効に利用することができるようになる。

【0022】さらに、請求項4に係る発明によれば、上記一方の機器はデジタルコンテンツ提供端末としてもよい。請求項5に係る発明によれば、上記一方の機器は携帯型情報端末としてもよい。請求項6に係る発明によれば、上記一方の機器は上記デジタルコンテンツを蓄積するユーザ端末としてもよい。

【0023】図5は、第1の機器と第2の機器の間で伝送されるデジタルコンテンツの入出力情報を管理するシステムの構成図である。請求項7に係る発明は、このようなシステムであって、上記第1の機器100に接続されたICカードリーダーライタ110と、上記ICカードリーダーライタ110に挿入され、上記デジタルコンテンツ130の上記入出力情報を格納する領域が設けられた耐タンパ性記憶領域310を有するICカード300とを更に有し、上記ICカードリーダーライタ110が接続された上記第1の機器100は、上記デジタルコンテンツの不正使用を防止するライセンス管理手段140を有し、上記ライセンス管理手段140は、上記第1の機器100と上記第2の機器200の間の上記デジタルコンテンツの伝送が許可されているかどうかを判定する手段142と、許可されていると判定された場合に、上記デジタルコンテンツの伝送を始動させ、上記デジタルコンテンツの伝送に応じた入出力情報を上記ICカードリーダーライタを介して上記ICカード300の耐タンパ性領域310に設定する手段144とを有することを特徴とする。

【0024】請求項7に係る発明によれば、実際にデジタルコンテンツがダウンロードされ、あるいは、蓄積される機器とは別個のICカード300にデジタルコンテンツの入出力情報を格納する領域が設けられるので、ICカード300が本質的に備えている耐タンパ性、安全性に起因して格納領域が不正にアクセスされる危険性が低減する。また、機器間でデジタルコンテンツの伝送を行なう際に、このICカードが接続されている機器からデジタルコンテンツの入出力情報を書き込むことができるので、ダウンロードされ、蓄積される側ではない方の機器を一方の機器として選択することによって、ダウンロードに利用された端末以外の端末をコンテンツ蓄積・管理端末として利用できるようになる。また、デジタルコンテンツを伝送する際に、そのデジタルコンテンツについての入出力情報をICカードに書き込むために直前に使用された機器とは異なる機器にそのICカードを接続し、今回の伝送に関する入出力情報をそのICカードに書き込むことによって、一つのコンテンツに対するコンテンツ蓄積・管理端末を変更することが可能である。

【0025】また、請求項8に係る発明は、デジタル

コンテンツを保持する第1の機器と、上記第1の機器から上記デジタルコンテンツを受ける第2の機器と、上記第1の機器と上記第2の機器の少なくとも一方の機器に接続されたICカードリーダーライタと、上記ICカードリーダーライタに挿入され、上記デジタルコンテンツの上記入出力情報を格納する領域が設けられた耐タンパ性記憶領域を有するICカードとを有するシステムにおいて、上記一方の機器で実行されるデジタルコンテンツの入出力情報管理プログラムを記録した記録媒体であって、上記第1の機器から上記第2の機器への上記デジタルコンテンツの伝送が不正使用であるかどうかを判定させるコードと、不正使用ではないと判定された場合に、上記デジタルコンテンツの伝送を始動させ、上記デジタルコンテンツの伝送に応じた入出力情報を上記ICカードリーダーライタを介して上記ICカードの耐タンパ性領域に設定させるコードとを有し、上記デジタルコンテンツの不正使用を防止することを特徴とするプログラムを記録した記録媒体である。

【0026】

20 【発明の実施の形態】以下、図6に示されるような本発明の第1実施例によるICカードを利用したコンテンツのチェックイン/チェックアウト管理システムを説明する。

【0027】同図には、コンテンツ取得・蓄積用機器であるパーソナルコンピュータ10、コンテンツ提供情報端末であるKIOSK端末60と、たとえば、インターネット上でコンテンツを配信することができるコンテンツサーバー40と、インターネットのようなコンピュータネットワーク50と、コンピュータネットワーク50に接続可能であり、コンピュータネットワーク50上のコンテンツを獲得することができる携帯端末70（たとえば、携帯電話機、PDAなど）と、CD-ROMプレーヤーのようなコンテンツ利用機器30とが示されている。

【0028】また、コンテンツのチェックイン/チェックアウト管理データを保持するために、第三者が参照・更新することが非常に困難であるICカード300の耐タンパ領域310が設けられる。従来技術において、機器内部に設けられた耐タンパ領域を使用してコンテンツのチェックイン/チェックアウト管理を行なっていたパーソナルコンピュータ10及びKIOSK端末60は、本実施例の場合、このICカード300上の耐タンパ領域310を使用することにより、コンテンツ管理用端末として働く。

【0029】そのため、本発明の第1実施例では、ICカード300の耐タンパ領域310に保持されたチェックイン/チェックアウト管理データにアクセスし、チェックイン/チェックアウト管理を行なうため、パーソナルコンピュータ10及びKIOSK端末60にはICカードリーダーライタが設けられる。

【0030】図6に示された本発明の第1実施例における構成要素の中で、図1乃至図4を参照して説明した従来技術のシステムの構成要素と同一若しくは同等のものには、同じ参照番号が付けられている。同図において、コンテンツは、KIOSK端末60のI/Oインタフェース65から利用機器30のI/Oインタフェース31へ、コンテンツサーバー40からコンピュータネットワーク50を介して携帯端末70のネットワークインタフェース71又はパーソナルコンピュータ10のネットワークインタフェース19に配信される。また、利用機器30のI/Oインタフェース31及び携帯端末70のI/Oインタフェース72と、パーソナルコンピュータ10のI/Oインタフェース17との間でもコンテンツを伝送することが可能である。

【0031】なお、ICカードリーダライタは、携帯端末70にも接続され、コンテンツサーバー40からコンピュータネットワーク50を介して携帯端末70にコンテンツをダウンロードする際に、コンテンツサーバー40がチェックイン/チェックアウト管理用端末としてチェックアウトデータを書き込むことができる。

【0032】本実施例では、実際にチェックイン/チェックアウト管理を行なうLCMは、パーソナルコンピュータ10と、KIOSK端末60と、コンテンツサーバー40とに設けられている。そのため、ICカード300の耐タンパ領域310のチェックイン・チェックアウトデータは、パーソナルコンピュータ10、KIOSK端末60、及び、ネットワークサーバー40からの指示によって書き込まれる。

【0033】図7は、本発明の第2実施例によるICカードの耐タンパ領域に記録されるチェックイン/チェックアウトデータを表形式で表わした図である。コンテンツIDは、このICカードのユーザがKIOSK端末あるいはコンテンツサーバーからダウンロードしたコンテンツ、又は、CD-ROMのようなメディアから読み出したコンテンツを識別するためのIDである。一つのコンテンツIDには、メディア/機器ID、及び、チェックイン/アウトフラグの二つの項目が関連付けられる。メディア/機器IDは、対応したコンテンツを取得した機器又はメディアを識別するためのIDである。チェックイン/アウトフラグは、対応したコンテンツを入力したのか、出力したのかを区別するフラグである。

【0034】同図の例では、1行目のコンテンツID="コンテンツ00"、メディア/機器ID="プレーヤーA"、チェックイン/アウトフラグ="アウト"は、コンテンツ00がプレーヤーAに出力されたことを表わす。また、2行目のコンテンツID="コンテンツ01"、メディア/機器ID="携帯端末B"、チェックイン/アウトフラグ="イン"は、コンテンツ01が携帯端末Bから入力されたことを表わす。3行目のコンテンツID="コンテンツ02"、メディア/機器ID

"メモリメディアC"、チェックイン/アウトフラグ="アウト"は、コンテンツ02がメモリメディアCに蓄積されたことを表わす。

【0035】図8は、本発明の第3実施例によるICカードと各端末間のチェックイン・チェックアウトデータの流れを示すタイミングチャートである。この例では、街頭などに設置されたKIOSK端末60から利用機器30にコンテンツを書き込み、次に、利用機器30からコンテンツ蓄積・管理用端末であるパーソナルコンピュータ10にそのコンテンツを書き込み、待避する場合を考える。また、本例では、機器の間でデータ通信されるコンテンツなどは、すべて暗号化(たとえば、周知の公開鍵暗号方式や秘密鍵暗号方式を用いて)されて通信経路を伝送される。

【0036】KIOSK端末60は、ICカードリーダライタ67と、ソフトウェアとして実装され得るコンテンツ管理用アプリケーションモジュール63及びLCM64を含む。ICカード300が挿入されていない状態では、KIOSK端末60は、チェックイン/チェックアウト管理用耐タンパ領域をもたないが、利用者がKIOSK端末60のICカードリーダライタ67にICカード300を挿入することで、コンテンツのチェックイン/チェックアウト管理用耐タンパ領域310がKIOSK端末60に対して提供される。

【0037】図8のステップ1からステップ7は、KIOSK端末60から利用機器30へのコンテンツの販売処理の手順を示している。利用者がICカード300をKIOSK端末60のICカードリーダライタ67に挿入すると、ICカードのチェックが行なわれる(ステップ1)。次に、利用者がKIOSK端末60に対し、コンテンツの書き込みを依頼すると、アプリケーションモジュール63がLCM64に対しコンテンツの書き込みを依頼し(ステップ2)、LCM63が利用機器30に対しコンテンツを書き込む(ステップ3)。利用機器30はコンテンツ書き込み完了をKIOSK端末60のLCM63に通知し(ステップ4)、LCM63はアプリケーションモジュールに完了通知を送る(ステップ5)。次に、KIOSK端末60のアプリケーションモジュール63は、ICカードリーダライタ67を介してICカード300の耐タンパ領域310にチェックアウトデータを書き込み(ステップ6)、続いて、書き込みデータを検査する(ステップ7)。

【0038】たとえば、利用者がKIOSK端末60から利用機器30(たとえば、機器ID="00A")に内蔵された記録媒体32などにコンテンツ(たとえば、コンテンツID="001")を取り込むと、ICカード300上の耐タンパ領域310には、コンテンツID="001"、メディア/機器ID="00A"、及び、チェックイン/アウトフラグ="アウト"が新たに書き込まれる。これは、コンテンツが利用機器へチェッ



クアウトされたことを表わす。これにより、KIOSK 端末 60 から利用機器 30 へのコンテンツの販売処理が完了する。

【0039】このときのチェックアウトデータの書き込みプロセスは、図 9 に示された本発明の第 4 実施例によるアプリケーションモジュールから IC カードへのチェックアウト時アクセスフローを参照して説明される。

【0040】ステップ 101：挿入された IC カードが不正なものでないかどうかを検査し、不正使用されている場合には、処理を終了する。

【0041】ステップ 102：IC カードが不正使用ではないので、IC カード内の耐タンパ領域を走査し、空き領域を確認する。

【0042】ステップ 103：チェックアウトされるべきコンテンツのコンテンツ ID と、移動先の記録媒体のメディア ID (若しくは機器 ID) を読み込む。

【0043】ステップ 104：取得したコンテンツ ID 及びメディア ID と、チェックアウトフラグを耐タンパ領域内の適当な部分に書き込む。

【0044】ステップ 105：チェックアウトデータの書き込みが正常に行なわれたかどうかを確認し、正常ではない場合、ステップ 103 に戻る。

【0045】ステップ 106：チェックアウトデータが正常に書き込まれているので、移動先の記録媒体などにコンテンツを転送する。

【0046】ステップ 107：コンテンツが正常に転送されたかどうかをチェックし、未だ転送が終了していない場合には、ステップ 106 に戻る。

【0047】ステップ 108：LCM は、コンテンツのコピーが禁止されている場合には、転送元のコンテンツを消去する。

【0048】利用機器 30 の記憶媒体 32 に取り込まれたコンテンツは、コンテンツ蓄積・管理用端末であるパーソナルコンピュータ 10 に待避されるまでの間は、利用機器 30 で利用することが可能である。

【0049】次に、再度図 8 を参照して、利用機器 30 に保持されているコンテンツをパーソナルコンピュータ 10 に待避するプロセスを説明する。

【0050】パーソナルコンピュータ 10 には、KIOSK 端末 60 と同様に、アプリケーションモジュール 14 及び LCM13 がインストールされ、IC カードリーダライタ 20 が接続される。利用者は、KIOSK 端末 60 でコンテンツを取得した際に利用した同じ IC カード 300 を IC カードリーダライタ 20 に挿入する。これにより、利用者は、KIOSK 端末 60 でのチェックイン/チェックアウト時に利用した IC カード 300 の耐タンパ領域 310 を、別の端末であるコンテンツ蓄積・管理用端末であるパーソナルコンピュータ 10 上でのコンテンツのチェックイン/チェックアウト管理用耐タンパ領域として利用できるようになる。ここで、利用さ

れている IC カード 300 上の耐タンパ領域 310 には、KIOSK 端末 60 から取得したコンテンツが利用機器 30 の記録媒体 32 にチェックアウトされていることを表わすデータが記録されている。

【0051】IC カード 300 が IC カードリーダライタ 20 に挿入されると、IC カード 300 の正当性検査が行なわれる (ステップ 8)。次に、パーソナルコンピュータ 10 のアプリケーションモジュール 14 は、移動させようとしているコンテンツが格納された利用機器 30 の記録媒体 32 の検査を LCM13 に依頼し (ステップ 9)、LCM13 はその記録媒体 32 を検査し (ステップ 10)、検査結果をアプリケーションモジュール 14 に返す (ステップ 11)。次に、アプリケーションモジュール 14 は、利用機器 30 の記録媒体 32 に格納されているコンテンツの検査を LCM13 に依頼し (ステップ 12)、LCM13 は利用機器 30 に対し記録媒体 32 に格納されているコンテンツのリストを要求する (ステップ 13)。利用機器 30 は、この要求に応じたコンテンツリストをパーソナルコンピュータ 10 の LCM13 に返答し (ステップ 14)、LCM13 はそのコンテンツリストをアプリケーションモジュール 14 に返す (ステップ 15)。

【0052】次に、アプリケーションモジュール 14 は、IC カード 300 の耐タンパ領域 310 にアクセスし、耐タンパ領域 310 に記録されているチェックアウトデータのチェックアウト情報を照合し、利用機器 30 から移動させようとしているコンテンツに関するチェックアウトデータを確認する (ステップ 16)。

【0053】続いて、アプリケーションモジュール 14 は、LCM13 に対しコンテンツの転送を要求し (ステップ 17)、LCM13 は、この転送が著作権保護の規定を満たしているならば、利用機器 30 に対しコンテンツの転送を要求する (ステップ 18)。要求を受けた利用機器 30 は、記録媒体 32 からコンテンツを取り出して転送し、パーソナルコンピュータ 10 の LCM13 に対し書き込みを依頼する (ステップ 19)。コンテンツの書き込みを依頼された LCM13 は、蓄積装置 16 にコンテンツを書き込む (ステップ 20)。

【0054】コンテンツの書き込み終了後、アプリケーションモジュール 14 は、(コピー禁止、移動のみ可の場合) LCM13 に対し転送元のコンテンツの消去を依頼し (ステップ 21)、LCM13 は利用機器 30 に対し記録媒体 32 に記憶されているコンテンツの消去を要求する (ステップ 22)。利用機器 30 は、コンテンツの消去処理の完了を LCM13 に通知し (ステップ 23)、LCM13 はこの完了通知をアプリケーションモジュール 14 に伝える (ステップ 24)。

【0055】最後に、パーソナルコンピュータ 10 のアプリケーションモジュール 14 は、IC カード 300 の耐タンパ領域 310 に記録されたチェックアウトフラグ



を消去してチェックインフラグに書き換える（ステップ 25）。

【0056】図 10 は、本発明の第 5 実施例によるアプリケーションモジュールから IC カードへのチェックイン時アクセスフローである。同図を参照して、チェックインデータの書き込みプロセスに付いて説明する。

【0057】ステップ 111：挿入された IC カードが不正なものでないかどうかを検査し、不正使用されている場合には、処理を終了する。

【0058】ステップ 112：チェックインされるべきコンテンツのコンテンツ ID と、移動元の記録媒体のメディア ID（若しくは機器 ID）を読み込む。

【0059】ステップ 113：IC カードが不正使用ではないので、IC カード内の耐タンパ領域を走査し、チェックインされるべきコンテンツに対応した領域を確認する。

【0060】ステップ 114：IC カードから読み出したチェックインデータと、コンテンツ自体のデータとが一致するかどうかを照合し、一致しない場合、プロセスを終了させる。

【0061】ステップ 115：対応するチェックアウトデータを消去して、チェックインデータに書き換える。

【0062】ステップ 116：チェックアウトデータが正常に消去されたかどうかを確認し、未だ消去されていない場合、ステップ 115 に戻る。

【0063】ステップ 117：正常にチェックアウトデータが消去されたので、コンテンツを転送する。

【0064】ステップ 118：コンテンツが正常に転送されたかどうかをチェックし、未だ転送が終了していない場合には、ステップ 117 に戻る。

【0065】ステップ 119：LCM は、コンテンツのコピーが禁止されている場合には、転送元のコンテンツを消去する。

【0066】パーソナルコンピュータ 10 に蓄積されているコンテンツは、LCM で禁止されていない限り、携帯端末 70 や利用機器 30 に再転送することが可能である。その場合、パーソナルコンピュータ 10 に接続されている IC カードリーダライタ 20 に IC カード 300 を挿入し、既に説明した KIOSK 端末 60 から利用機器 30 へのコンテンツのダウンロードと同様の処理を行なうことにより、パーソナルコンピュータ 10 から携帯端末 70 又は利用機器 30 にコンテンツを移動し、このコンテンツのチェックイン・チェックアウトデータを書き換えることができる。正常に転送ができた場合には、パーソナルコンピュータ 10 に蓄積されていたコンテンツが消去される。

【0067】本発明の第 6 実施例では、コンテンツサーバー 40 からコンピュータネットワーク 50 を介して携帯端末 70 にコンテンツが配信される。この場合、携帯端末 70 に接続された IC カードリーダライタ 75 に I

C カード 300 を挿入することにより、既に説明したチェックイン/チェックアウト管理と同様の処理を行なうて、コンテンツを携帯端末 70 に書き込み、IC カード 300 の耐タンパ領域 310 のチェックイン/チェックアウトデータを書き換えることができる。このとき、コンテンツサーバー 40 の LCM 43 は、携帯端末 70 のアプリケーションモジュール 74 を介してチェックアウトデータを IC カード 300 の耐タンパ領域 310 に書き込むことに注意する必要がある。たとえば、利用者がコンテンツサーバー 40 から携帯端末 70（たとえば、機器 ID="00B"）に内蔵された記録媒体 73 などにコンテンツ（たとえば、コンテンツ ID="002"）を取り込むと、IC カード 300 上の耐タンパ領域 310 には、コンテンツ ID="002"、メディア/機器 ID="00B"、及び、チェックイン/アウトフラグ="アウト" が新たに書き込まれる。また、このコンテンツをパーソナルコンピュータ 10 に待避させ、パーソナルコンピュータ 10 で管理するためには、この IC カード 300 をコンテンツ蓄積・管理用端末であるパーソナルコンピュータ 10 の IC カードリーダライタ 20 に挿入し、携帯端末 70 の記録媒体 73 に書き込まれたコンテンツをパーソナルコンピュータ 10 に転送し、携帯端末 70 の記録媒体 73 上のコンテンツを消去し、チェックイン/アウトフラグを"イン"書き換えればよい。

【0068】また、上記の本発明の実施例によるチェックイン/チェックアウト管理システムの構成は、上記の実施例で説明された例に限定されことなく、システム内のの入出力デバイス、通信デバイス、IC カード、IC カードリーダライタ、コンピュータの CPU やメモリなどのハードウェア部分を除く部分は、同等の機能を実現するソフトウェア（プログラム）で構築し、ディスク装置等に記録しておき、必要に応じてコンピュータにインストールしてチェックイン/チェックアウト管理を行うことも可能である。さらに、構築されたプログラムをフロッピー（登録商標）ディスク、メモ리카ード、CD-ROM 等の可搬記録媒体に格納し、このような情報検索処理を用いる場面で汎用的に使用することも可能である。

【0069】以上、本発明の代表的な実施例を説明したが、本発明は、上記の実施例に限定されことなく、特許請求の範囲内において、種々変更・応用が可能である。

【0070】

【発明の効果】以上の説明の通り、従来ではコンテンツを取得した端末、若しくは、コンテンツを格納したコンテンツ蓄積・管理端末のみでチェックイン/チェックアウト管理が行なわれていたのに対し、本発明により、IC カードの耐タンパ領域にチェックイン/チェックアウト情報を格納し利用することで、チェックイン/チェッ

クアウト情報へのアクセスがロケーションフリーになるので、ＩＣカードリーダライタを具備し、かつ、チェックイン／チェックアウト管理用ソフトウェアがインストールされている全ての端末をコンテンツ蓄積・管理端末として使用することが可能になる。

【００７１】また、従来は、一つのコンテンツに対して一つのコンテンツ蓄積・管理用端末を対応付ける必要があったが、本発明によれば、コンテンツのチェックイン／チェックアウト情報がＩＣカードに格納されているので、このコンテンツに対するコンテンツ蓄積・管理用端末は、ＩＣカードをリード／ライトできる装置に自由に変更することができる。

【００７２】したがって、本発明によれば、ＬＣＭの規定の範囲内でコンテンツを機器間で自由に移動し、若しくは、コピーすることが可能になる利点が得られる。

【００７３】また、従来、チェックイン・チェックアウト情報は、コンテンツ蓄積・管理用端末内のハードウェア若しくはソフトウェア上での耐タンパ領域に格納していた。これに対し、本発明によれば、チェックイン・チェックアウト情報がＩＣカードの耐タンパ領域に格納されているので従来技術よりも高い安全性が実現される。なぜならば、ＩＣカードは、（１）カード自体を物理的に複製することが非常に困難である、（２）カード内部へのアクセスが難しく、データの改竄や盗み見が難しい、（３）カードとリーダライタの間で、各々の正当性をローカルで認証することができ、不正利用、不正カードを検出し易い、などの優れた特性を備えているからである。

【図面の簡単な説明】

【図１】従来技術によるＣＤリップングシステムの構成図である。

【図２】従来技術によるネットワーク経由でコンテンツをダウンロードするシステムの構成図である。

【図３】従来技術によるコンテンツ提供情報端末からのコンテンツ取得システムの構成図である。

【図４】従来技術による携帯端末を利用したネットワーク経由のコンテンツ取得システムの構成図である。

【図５】本発明によるデジタルコンテンツ入出力情報管理システムの構成図である。

【図６】本発明の第１実施例によるＩＣカードを利用したコンテンツのチェックイン／チェックアウト管理システムの構成図である。

【図７】本発明の第２実施例によるＩＣカードの耐タンパ領域に記録されるチェックイン／チェックアウトデータの説明図である。

【図８】本発明の第３実施例によるＩＣカードと各端末間のチェックイン・チェックアウトデータの流れを示すタイミングチャートである。

【図９】本発明の第４実施例によるアプリケーションモジュールからＩＣカードへのチェックアウト時アクセスフローチャートである。

【図１０】本発明の第５実施例によるアプリケーションモジュールからＩＣカードへのチェックイン時アクセスフローチャートである。

【符号の説明】

- １００ 第１の機器
- １１０ ＩＣカードリーダライタ
- １２０、２１０ Ｉ／Ｏインタフェース
- １３０、２３０ デジタルコンテンツ
- １４０ ライセンス管理手段
- １４２ 伝送許可判定手段
- １４４ 耐タンパ領域設定手段
- ２００ 第２の機器
- ３００ ＩＣカード
- ３１０ 耐タンパ性記憶領域

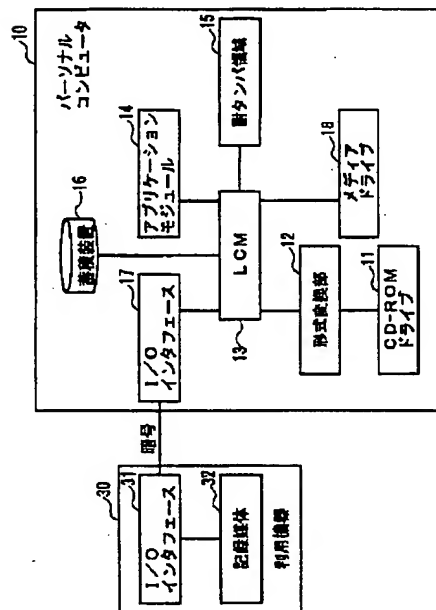
【図 7】

本発明の第2実施例によるＩＣカードの耐タンパ領域に記録されるチェックイン／チェックアウトデータの説明図

コンテンツID	メディア/機器ID	チェックイン/ チェックアウト
コンテンツ00	プレイヤーA	アウト
コンテンツ01	携帯端末B	イン
コンテンツ02	メモリメディアC	アウト
⋮	⋮	⋮

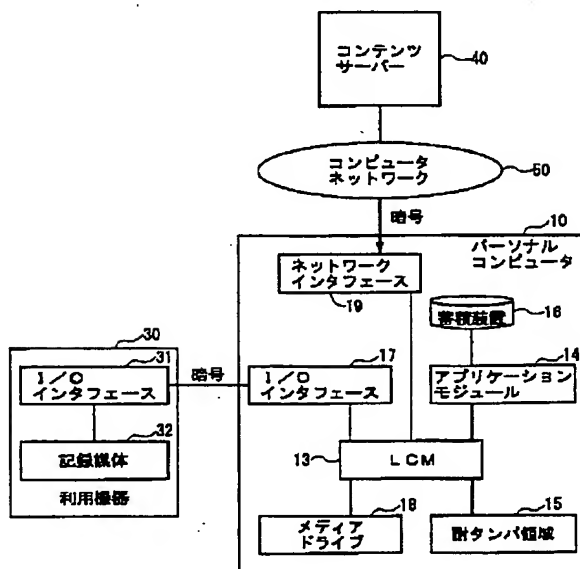
【図1】

従来技術によるCDリッピングシステムの構成図



【図2】

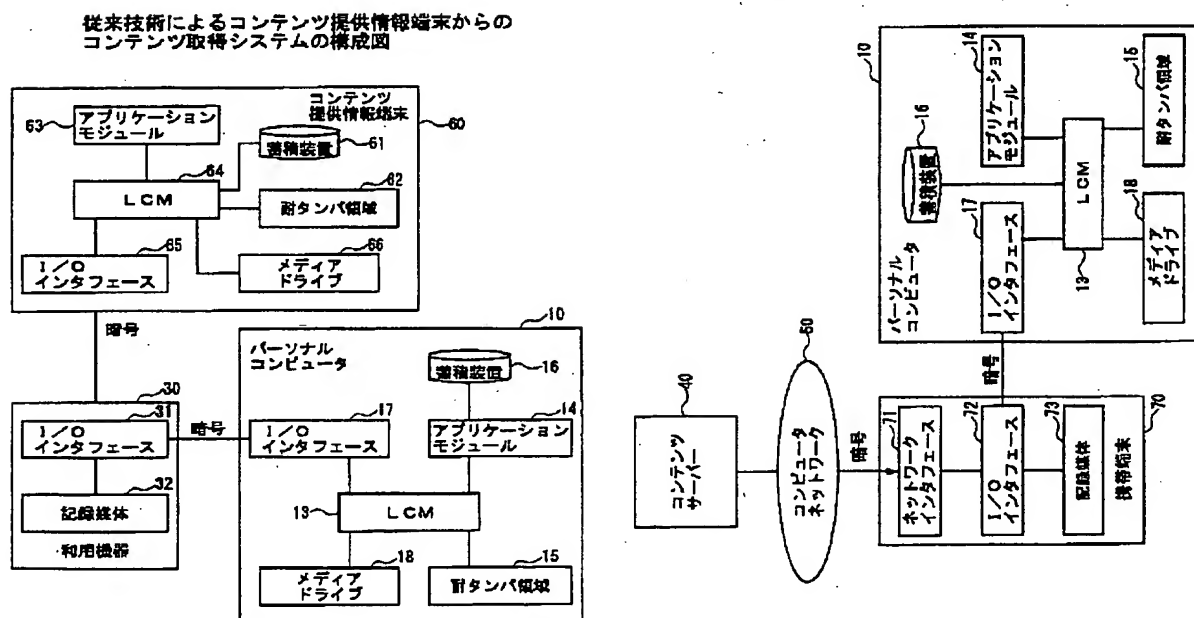
従来技術によるネットワーク経由でコンテンツをダウンロードするシステムの構成図



【図4】

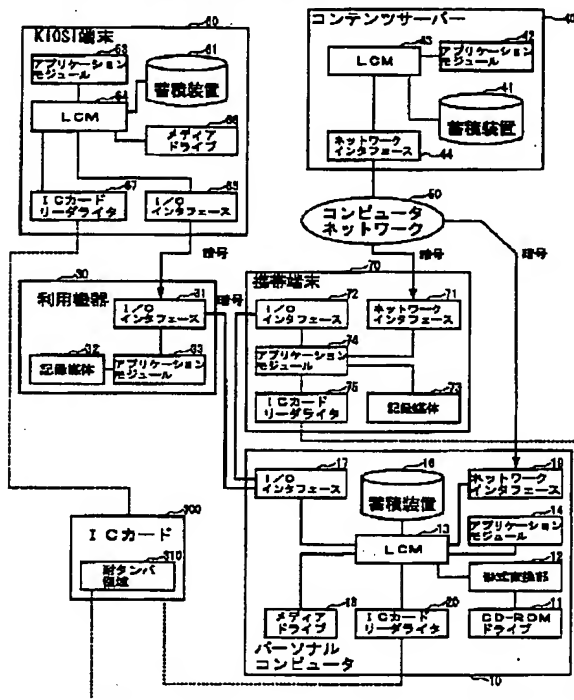
【図3】

従来技術による携帯端末を利用したネットワーク経由のコンテンツ取得システムの構成図



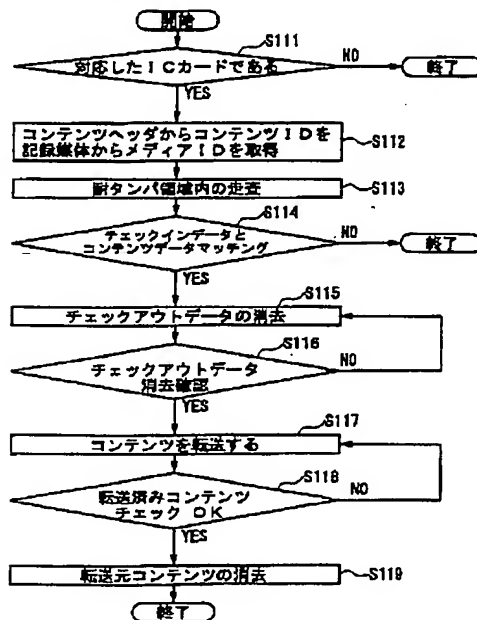
【图 6】

本発明の第1実施例によるICカードを利用したコンテンツの  
チェックイン/チェックアウト管理システムの構成図

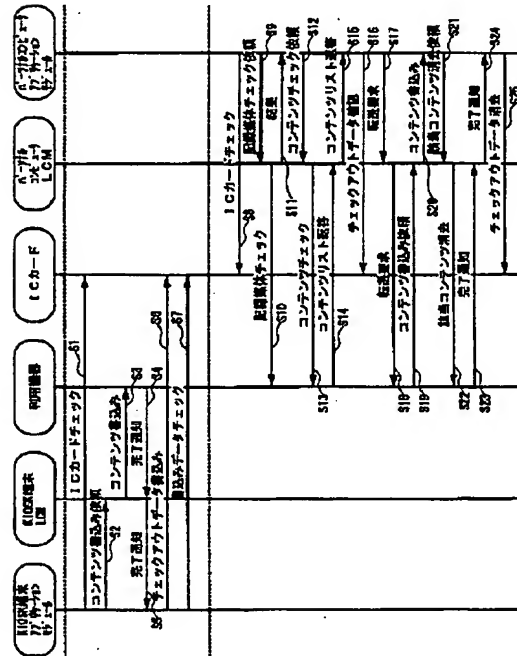


【图 10】

本発明の第5実施例によるアプリケーションモジュールからICカードへのチェックイン時アクセスフローチャート



本発明の第3実施例によるICカードと各端末間のチェックイン・チェックアウトデータの流れを示すタイミングチャート



(51) Int. Cl. <sup>7</sup>	識別記号	F I	テマコード* (参考)
G 0 6 K 17/00		G 0 6 K 17/00	L
			D
19/07		G 0 9 C 1/00	6 6 0 D
G 0 9 C 1/00	6 6 0	G 0 6 K 19/00	N
H 0 4 L 9/10		H 0 4 L 9/00	6 2 1 Z
9/32			6 7 3 E
			6 7 3 B

(72) 発明者 荒木 秀教  
東京都千代田区内幸町一丁目1番6号 エヌ・ティ・ティ・コミュニケーションズ株式会社内

Fターム(参考) 5B035 AA13 BB09 BC00  
5B049 AA05 BB00 CC00 FF08 GG02  
GG10  
5B058 CA27 KA02 KA04 KA31 YA20  
5B085 AA08 AE00 BC02  
5J104 AA07 AA13 KA02 NA35 NA42